Estructuras Algebraicas Segundo examen parcial	1er Apellido: __________	24 de mayo de 2016
Departamento Matem. aplic. TIC ETS de Ingenieros Informáticos Universidad Politécnica de Madrid	2º Apellido: __________ Nombre: __________ Número de matrícula:	Tiempo 2 h. **Calificación:**

Comprueba que las dos hojas grapadas del examen, están impresas a doble cara.

1. (2,5 puntos)

a) Sea $(R, +, \cdot)$ un anillo y sea $S \subseteq R$. ¿Qué propiedades debe verificar S para ser un subanillo de R?

i) $S \neq \emptyset$

ii) $\forall a, b \in S \quad a-b \in S$ y $a \cdot b \in S$

b) Demostrar que $T = \{\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} : a \in \mathbb{Q}\}$ es un subanillo de $(\mathbb{Q}^{2\times 2}, +, \cdot)$. ¿Es un ideal?

i) $T \neq \emptyset$ porque $0 \in \mathbb{Q} \Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$

ii) $\forall \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} \in T$ es $a, b \in \mathbb{Q} \Rightarrow a-b,\ a\cdot b \in \mathbb{Q} \Rightarrow$

$\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ -a+b & 0 \end{pmatrix} \in T$ y $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} \in T$

$\Rightarrow T$ es subanillo de $\mathbb{Q}^{2\times 2}$

T no es ideal: $\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix} \notin T$

c) ¿Es T un subanillo conmutativo? Marca la opción correcta y justifica la respuesta:

Sí   T es subanillo conmutativo:

No $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}$

d) ¿Es T un cuerpo? Marca la opción correcta y justifica la respuesta:

Sí   T es cuerpo: Es conmutativo, tiene identidad

No $e = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}$ ($\begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}$) y es de división:

$\forall \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T$ con $\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ es $a \in \mathbb{Q}$ con $a \neq 0 \Rightarrow$

$\exists \frac{1}{a} \in \mathbb{Q} \Rightarrow \begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix} \in T$ y $\begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{1}{a} & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 0 \end{pmatrix} = e$

e) Estudiar si T es isomorfo a $(\mathbb{Q}, +, \cdot)$ Sea $\varphi : T \longrightarrow \mathbb{Q}$ $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = a$

i) φ está bien definida y es biyectiva:

- $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) \Leftrightarrow a = b \Leftrightarrow \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}$
- $\forall a \in \mathbb{Q} \quad \exists \begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} \in T$ tq $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) = a$

ii) φ es homomorfismo de anillos:

- $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} a+b & 0 \\ -a-b & 0 \end{pmatrix}) = a+b = \varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}) + \varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix})$
- $\varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix}) = \varphi(\begin{pmatrix} ab & 0 \\ -ab & 0 \end{pmatrix}) = ab = \varphi(\begin{pmatrix} a & 0 \\ -a & 0 \end{pmatrix})\,\varphi(\begin{pmatrix} b & 0 \\ -b & 0 \end{pmatrix})$

2. (2,5 puntos) Los siguientes conjuntos, con las operaciones usuales en cada uno de ellos, son anillos conmutativos con identidad:

$$R_1 = \mathbb{Z}_5, \qquad R_2 = \mathbb{Z}_6 \times \mathbb{Z}_4, \qquad R_3 = \mathbb{Z}[x], \qquad R_4 = \{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Q}\}$$

a) Dar la identidad de cada uno de los anillos citados:

Identidad de R_1	Identidad de R_2	Identidad de R_3	Identidad de R_4
$\{1\}_5 = 1$ Notación	$(\{1\}_6, \{1\}_4) =$ notación $(1, 1)$	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

b) Encontrar la característica de cada uno de los anillos citados:

Característica de R_1	Característica de R_2	Característica de R_3	Característica de R_4
5	12	0	0

c) Describir las unidades de cada uno de los anillos

Unidades de R_1	Unidades de R_2	Unidades de R_3	Unidades de R_4
$\{1, 2, 3, 4\}$	$\{(1,1), (1,3), (5,1), (5,3)\}$	$\{1, -1\}$	$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $\forall a, b \in \mathbb{Q}^*$

d) Indicar si el anillo correspondiente tiene divisores de cero. En caso afirmativo dar un ejemplo.

Divisor de cero en R_1	Divisor de cero en R_2	Divisor de cero en R_3	Divisor de cero en R_4
No tiene	Sí tiene, por ejemplo $(3, 2)$	No tiene	Sí tiene, por ejemplo $\begin{pmatrix} 7 & 0 \\ 0 & 0 \end{pmatrix}$

e) ¿Es alguno de ellos dominio de integridad? ¿Es alguno de ellos cuerpo?
En caso afirmativo indicar cuáles. Justificar la respuesta

Son dominios de integridad R_1 y R_3
(conmutativos, con identidad y sin divisores de cero)

Es cuerpo: R_1
(dominio de integridad de división)

3. (2,5 puntos)

a) Estudiar si $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ es una extensión simple de $\mathbb{Q}$. $\mathbb{Q}(\sqrt{2}+\sqrt{6}) = \mathbb{Q}(\sqrt{2}, \sqrt{6})$

"$\subseteq$" $\sqrt{2}+\sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{6})$

"$\supseteq$" $\sqrt{2}+\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{6}) \Rightarrow (\sqrt{2}+\sqrt{6})^2 = 8 + 4\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{6}) \Rightarrow$

$\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{6}) \Rightarrow \sqrt{3}(\sqrt{2}+\sqrt{6}) = \sqrt{6} + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{6}) \Rightarrow$

$(\sqrt{6}+3\sqrt{2}) - (\sqrt{2}+\sqrt{6}) = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{6}) \Rightarrow \underline{\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{6})}$

$\Rightarrow (\sqrt{2}+\sqrt{6}) - \sqrt{2} = \underline{\sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{6})}$

$\Rightarrow$ $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ es una extensión simple

b) Se considera el polinomio $p = x^4 - 2x^3 + 6x - 10 \in \mathbb{Q}[x]$. Demostrar que es irreducible.

Por el criterio de Eisenstein: $2 \in \mathbb{N}$ es primo y divide a todos los coeficientes salvo al principal, y $2^2 = 4$ no divide al coeficiente de grado cero.

c) El teorema de Kronecker garantiza la existencia de una raíz α de p. ¿En qué cuerpo asegura el teorema de Kronecker que existe una raíz de p?

$$\mathbb{Q}[x]/\langle p \rangle \approx \mathbb{Q}(\alpha)$$

d) En el cuerpo y para la raíz α citados en el apartado anterior, realizar las siguientes operaciones:

1) $(\alpha^2 - 1)(\alpha^2 - \alpha + 1)$

$$\alpha^4 - \alpha^3 + \alpha - 1 = \underline{\alpha^3 - 5\alpha + 9}$$

2) $(\alpha^2 - 2\alpha + 3)^{-1}$

$x^4 - 2x^3 + 6x - 10$		$(1, 0)$
$x^2 - 2x + 3$	$x^2 - 3$	$(0, 1)$
-1		$(1, 3 - x^2)$

$$\Rightarrow (\alpha^2 - 2\alpha + 3)^{-1} = \underline{\alpha^2 - 3}$$

4. (2,5 puntos)

a) Calcular el polinomio mínimo de $\beta = \sqrt[3]{2} + \sqrt[3]{4}$ sobre $\mathbb{Q}$.

$B = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, $f: \mathbb{Q}(\beta) \longrightarrow \mathbb{Q}(\beta)$

$f(x) = \beta x$

$$M = \begin{pmatrix} 0 & 2 & 2 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}$$

$P_M(\lambda) = -\lambda^3 + 6\lambda + 6$

$\Rightarrow$ El polinomio pedido es

$\underline{x^3 - 6x - 6}$

b) Calcular una base y el grado de extensión de $\mathbb{Q}(\sqrt{5}, \sqrt[6]{5})$ sobre $\mathbb{Q}$.

$B = \{1, 5^{1/6}, \underset{\parallel}{5^{2/6}}, \underset{\parallel}{5^{3/6}}, \underset{\parallel}{5^{4/6}}, 5^{5/6}\}$

$\phantom{B = \{1, 5^{1/6},} 5^{1/3} \quad 5^{1/2} \quad 5^{2/3}$

$[\mathbb{Q}(\sqrt{5}, \sqrt[6]{5}) : \mathbb{Q}] = 6$

c) Demostrar que $h = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ es irreducible en $\mathbb{Z}_2[x]$.

h es un polinomio de grado 3 y no tiene raíces en $\mathbb{Z}_2$ $\Rightarrow$ h es irreducible

d) Estudiar si h es un polinomio primitivo. Justificar la respuesta.

En $\mathbb{Z}_2[x]/\langle h \rangle$

$\langle x \rangle = \{1, x, x^2, x^3 = x^2+1, x^4 = x^2+x+1, x^5 = x+1, x^6 = x^2+x\}$

$\Rightarrow$ h es primitivo

e) Indicar qué elementos del cuerpo $\mathbb{Z}_2[x]/\langle h \rangle$ tienen raíz cuadrada.

$0 = 0^2$

$1 = 1^2$

$x = x^8 = (x^2+x+1)^2$

$x+1 = x^{12} = (x^2+x)^2$

$x^2 = (x)^2$

$x^2+1 = x^{10} = (x+1)^2$

$x^2+x = x^6 = (x^2+1)^2$

$x^2+x+1 = x^4 = (x^2)^2$

$\Rightarrow$ Todo elemento de $\mathbb{Z}_2[x]/\langle h \rangle$ tiene raíz cuadrada